

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK-----X
:
UNITED STATES OF AMERICA,
:-v-
:JOSHUA ADAM SCHULTE,
:Defendant.
:
-----X

17-CR-548 (JMF)

MEMORANDUM OPINION
AND ORDER

JESSE M. FURMAN, United States District Judge:

In this case, familiarity with which is presumed, Defendant Joshua M. Schulte, a former employee of the Central Intelligence Agency, is charged with stealing national defense information (“NDI”) and transmitting it to WikiLeaks as well as disclosing and attempting to disclose NDI while detained pending trial at the Metropolitan Correctional Center (“MCC”). *See* ECF No. 405 (“S3”). A first trial before Judge Paul A. Crotty ended in a conviction on two counts and a mistrial on the others; retrial is scheduled for June 13, 2022. On January 28, 2022, Defendant filed five pretrial motions. *See* ECF No. 765 (“Def.’s Omnibus Mem.”). On April 29, 2022, the Court issued an Opinion addressing three of those motions. *See* ECF No. 789. The Court then issued a separate order denying part of Defendant’s fourth motion. *See* ECF No. 794.

This Opinion addresses the remaining portions of Defendant’s third and fourth pretrial motions, both of which pertain to forensic evidence. In particular, Defendant moves (1) to preclude the Government from introducing forensic evidence to which Defendant and his expert did not have access, *see* Def.’s Omnibus Mem. 40-46, and (2) to compel the production of certain forensic evidence, including “the CIA’s Stash and Confluence backups that were allegedly stolen and transmitted to WikiLeaks,” *see id.* at 46-51. Significantly, this is not the first time Defendant has sought such relief. He moved for access to additional forensic discovery

both before and after the first trial, and those motions were denied by Judge Crotty after an extensive process under the Classified Information Procedures Act (“CIPA”), 18. U.S.C. app. 3. *See United States v. Schulte*, 2019 WL 3764662 at *5 (S.D.N.Y. July 22, 2019) (ECF No. 124) (granting in part the Government’s CIPA Section 4 Motion and denying Defendant’s request for “a complete forensic copy of the Schulte Workstation and DevLAN”); *United States v. Schulte*, 2021 WL 4335723, at *1 (S.D.N.Y. Sept. 23, 2021) (ECF No. 514) (denying Defendant’s renewed request, after the first trial, for “full ‘mirror’ images of the CIA’s ESXi and FSO1 (‘NetApp’) servers”).

After reviewing the parties’ initial submissions, the Court ordered the parties to file expert affidavits regarding the forensic discovery that had already been produced and the need for any additional discovery. ECF No. 767; *see* ECF No. 787-1 (“Bellovin Aff.”); ECF No. 791-1 (“Leedom Aff.”); ECF No. 791-2 (“Berger Aff.”). The Court also ordered the Government to submit a record of the classified discovery produced to Defendant. *See* ECF No. 795. Having reviewed those submissions, the Court denies Defendant’s remaining motions for the reasons that follow.

A. Motion to Preclude

Defendant argues that because he and his expert do not have access to the complete forensic images of the CIA servers that the Government provided to its own experts, any reliance on information obtained from those images should be precluded. In particular, Defendant argues that he has a constitutional right to reciprocal discovery and to effective cross examination of the Government’s experts, and that both rights require granting him equal access to all forensic discovery or precluding the Government from using that information. The Court is not persuaded.

Beginning with the question of reciprocal discovery, it is true that the Supreme Court has recognized such a right in some circumstances. *See Wardius v. Oregon*, 412 U.S. 470, 475

(1973) (striking down a statute requiring a defendant to give notice of an alibi without providing for reciprocal discovery). Notably, however, that right has been established in the context of rules that require a defendant to produce information without placing the same burden on the prosecution. *See id.*; *United States v. Bahamonde*, 445 F.3d 1225, 1229 (9th Cir. 2006) (reversing a conviction where the defendant was not allowed to admit a government agent’s testimony because he failed to comply with a government regulation requiring him to disclose the relevance of the testimony sought before trial, where there was no reciprocal obligation on the government). That is wholly different than the argument Defendant makes here, which is that the Government must provide Defendant with any forensic information in its possession.

But even assuming that *Wardius* applies under these circumstances, the Court has explicitly determined that reciprocal discovery is a limited right, which applies only “in the absence of a strong showing of state interests to the contrary.” 412 U.S. at 475. Here, there can be no question that the Government has a strong interest in maintaining the confidentiality of classified information such as that contained in the CIA servers. *See Schulte*, 2019 WL 3764662, at *6 (“Complete forensic copies of the Schulte Workstation and DevLAN would contain a tremendous amount of classified information. . . . Granting [Defendant] unfettered access . . . would gut the entire rationale behind CIPA.”). For that reason, the cases Defendant cites — none of which involved CIPA — are inapposite. *See* Def.’s Omnibus Mem. 41 (citing *United States v. Shrake*, 515 F.3d 743, 747 (7th Cir. 2008), *Barnard v. Henderson*, 514 F.2d 744, 745 (5th Cir. 1975)). Indeed, “courts have consistently and sensibly rejected the argument that CIPA is unconstitutional under *Wardius*” for precisely that reason. *United States v. Rosen*, 518 F. Supp. 2d 798, 801 (E.D. Va. 2007) (collecting cases); *cf. United States v. Bin Laden*, No. 98-CR-1023 (LBS), 2001 WL 66393, at *5 (S.D.N.Y. Jan. 25, 2001), *aff’d sub nom. In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93 (2d Cir. 2008). Put simply, because “CIPA is designed to protect important classified national security information,” it “entails the kind of

strong state interest that may justify an exchange of information between the prosecution and the defense that is not entirely reciprocal.” *Rosen*, 518 F. Supp. 2d at 801 (cleaned up).

Defendant’s argument pursuant to the Sixth Amendment’s Confrontation Clause is no more persuasive. Defendant argues that he cannot effectively cross-examine the Government’s experts without access to all of the information to which they had access. To begin with, “the right to confront and to cross-examine is not absolute and may, in appropriate cases, bow to accommodate other legitimate interests in the criminal trial process.” *Chambers v. Mississippi*, 410 U.S. 284, 295 (1973). Many courts have rejected Confrontation Clause challenges to CIPA on the grounds that it deprives a defendant of effective cross-examination. *See Bin Laden*, 2001 WL 66393, at *5 (rejecting a challenge to CIPA on the ground that the defendant’s counsel might be unable to identify classified information needed for cross-examination *ex ante*); *United States v. Lee*, 90 F. Supp. 2d 1324, 1328 (D.N.M. 2000) (rejecting a challenge to CIPA on the ground that it requires a defendant to preview his cross examination prior to trial). But more fundamentally, the Court is not persuaded that Defendant lacks any information he would need to effectively cross-examine the Government’s experts. As discussed more fully in the following section of this Opinion, the Government represents that it has provided Defendant or his expert with everything that the Government’s experts rely on in their analyses. *See* ECF No. 761 (“Gov.’s Omnibus Opp’n”), at 37 (“The Government has complied with its disclosure obligations by providing the defendant with all of the facts and data upon which [Leedom] based his opinions.”); ECF No. 791 (“Gov.’s Letter”), at 4 (“[T]he defense now has access to the exact same material that [Berger] used to conduct his analysis.”); Berger Decl. ¶¶ 6, 12, 18; Leedom Decl. ¶ 5. That is more than enough for Defendant to effectively cross-examine the Government’s experts. For both reasons, the Confrontation Clause offers no basis for granting Defendant’s motion to preclude.

B. Motion to Compel

As noted above, Judge Crotty twice denied Defendant's motions for additional forensic discovery, both before and after the first trial, and concluded that the Government could withhold certain forensic information pursuant to CIPA Section 4. In the first decision, Judge Crotty left open the possibility of ordering additional discovery, if Defendant "submit[ed] a more tailored request and provide[d] good reason for further forensic discovery." *Schulte*, 2019 WL 3764662, at *6. Defendant contends that his most recent motion — for "access to the CIA's Stash and Confluence backups that were allegedly stolen and transmitted to WikiLeaks" — is such a "tailored" request. Def.'s Omnibus Mem. 47. Notably, however, Defendant's request is a moving target. Elsewhere in his motion he argues that, because "Wikileaks published information that the government alleged derived from both Confluence and Stash, Mr. Schulte must be allowed access to those backups; however, Mr. Schulte is entitled not only access to the two specific backups the government alleges Mr. Schulte stole, but also access to all the Stash and Confluence backup files in the CIA's possession." *Id.* at 49. And his reply memorandum in support of his expert affidavit goes further still, asking for "the government to produce the complete 'mirror images' of the Schulte Workstation, ESXi Server, [and] FSO1 Server," ECF No. 793 ("Def.'s Reply"), at 8 — the exact request that Judge Crotty previously denied. The Court will confine its analysis to Defendant's original request in his motion, for access to the "Stash and Confluence backups that were allegedly stolen and transmitted to WikiLeaks." As to that issue, Defendant's motion must be and is denied, because nearly all of the information he seeks has already been provided, and he has not shown how additional information would be "helpful or material to the defense." *United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008).

Beginning with the Confluence backup, Defendant's expert has had access to "unredacted copies of the March 2 and 3, 2016 . . . backups" via a laptop at the CIA. Leedom Aff. ¶ 8. It is the March 3, 2016 backup that the Government alleges was stolen. Gov.'s Letter 4.

Accordingly, Defendant's expert has access, via the CIA laptop, to the exact material Defendant seeks in his motion: the "[March 3, 2016] Confluence backup[]" that w[as] allegedly stolen and transmitted to WikiLeaks." Def.'s Omnibus Mem. 47. Although Defendant's expert contends that he was permitted to spend only a few hours reviewing the files on the CIA laptop, Bellovin Aff. ¶ 16, they have long been available, and "remain[] available," to him, Leedom Aff. ¶ 9.¹ In addition, Defendant and his expert have direct access to "redacted Confluence backups" from March 3 and 4, 2016, Bellovin Aff. ¶ 15, and April 25, 2016, Gov.'s Letter 4. The Government has also agreed to produce an unredacted copy of the April 25, 2016 backup — the most recent backup available — to the defense via the CIA computer. *Id.*² Because the Government's expert relied solely on the April 25, 2016 backup, and certain data from the March 2, 3, and 4, 2016 backups, with that latest production, "the defense now has access to the exact same material that Mr. Berger used to conduct his analysis." Gov.'s Letter 4.

Turning to the Stash backup, Defendant's expert has access, via the CIA laptop, to "unredacted copies of the Stash repositories for any CIA tool for which source code has been released by WikiLeaks," "unredacted copies of all Stash documentation that has been released by WikiLeaks," and "all Stash commit logs for all projects released by WikiLeaks," which redact only the usernames of the individuals who saved particular versions of those products. Leedom Aff. ¶ 8. Thus, although Defendant's expert does not have access to the complete Stash backup,

¹ Moreover, to the extent Defendant's expert contends that he may need to look things up on the Internet during his analysis and is unable to do so at the CIA facility, Bellovin Aff. ¶¶ 16, 37, he may schedule multiple sessions to review the materials on the CIA laptop, with time in between to conduct research.

² Defendant contends that having access to "the most recent backup" is the same thing as "relying upon all [the] backups" because "the most recent backup contains the data from all previous backups." Def.'s Reply 2. If so, it is difficult to see why the Confluence issue is not put to rest by the Government's new production of an unredacted copy of the most recent Confluence backup. (Why the Government made that production only now, more than four years into the case, is a different matter that the Government does not address.)

he does have access to backups of the material that WikiLeaks has released.³ That is precisely the material the Government's expert relied on in his analysis. Berger Aff. ¶¶ 7-12.

In short, Defendant's expert appears to have access to nearly all of the information Defendant seeks in his motion. To the extent Defendant seeks access to the complete Stash backup, and currently has access only to the Stash repositories for any CIA tool for which source code has been released by WikiLeaks, Defendant's expert affidavit does not show why further information would be "helpful and material to the defense." *Aref*, 533 F.3d at 80. Perhaps most relevantly, Defendant's expert contends that he is unable to reproduce the Government expert's "timing analysis" — demonstrating when the data leaked to WikiLeaks was stolen — without full access to both backups. Bellovin Aff. ¶ 17. But notably, the Government's expert represents he did not even use the backups to conduct his timing analysis, Berger Aff. ¶¶ 7-11, and that all the materials that he did use were made available to Defendant's expert, *id.* ¶ 12. Indeed, as to the Stash repositories for the tools not released by WikiLeaks, those repositories "would be of no value or relevance . . . [to a timing analysis] since there would be no point of comparison from WikiLeaks to determine whether" a specific file was the one that had been leaked. *Id.*

Finally, to the extent that Defendant, through his motion papers or his expert's declaration, seeks once again to gain access to the full mirror images of the relevant servers, as opposed to making a more tailored request, the Court is not persuaded that his arguments justify

³ The Government's letter states that "[t]here does not appear to be any dispute that the Government has already produced to the defendant and to his expert the March 3, 2016 backups that the Government alleges were stolen and transmitted to WikiLeaks." Gov.'s Letter 3-4. But there is a dispute as to whether Defendant has access to the complete Stash backup (as opposed to particular Stash repositories). *See* Def.'s Reply 4 ("The government never provided the Stash backup."). Moreover, the December 10, 2018 Classified Discovery Letter to which the Government cites appears to support Defendant's position, that the Government has provided the March 3, 2016 Confluence backup, but *not* the complete March 3, 2016 Stash backup in its entirety. *See* December 10, 2018 Classified Discovery Letter, at 2-5; *see also* November 5, 2019 Classified Discovery Letter (explaining that the Stash backup made available via the CIA laptop would include only data for tools that WikiLeaks had disclosed, i.e., not the entire backup).

revisiting Judge Crotty’s prior rulings on this issue. Defendant’s expert speculates about exculpatory evidence he might find if given access to the full range of forensic discovery in the Government’s possession, but he offers no reason to believe any of that evidence actually exists. *See Bellovin Aff.* ¶¶ 19, 21, 24, 35, 38-39.⁴ It is certainly true that the forensic data is of critical importance to the Government’s case when it comes to the WikiLeaks charges. But as discussed above, Defendant has been granted access to a vast amount of forensic data — including all of the data on which the Government’s case will rest. Defendant has not “provide[d] good reason for further forensic discovery” that would justify “ordering production of forensic data beyond what supports the Government’s own theory of the case.” *Schulte*, 2019 WL 3764662, at *6.

Finally, Defendant argues that it is not enough for the Government to have made the forensic data available to his expert. He contends that *he* personally is entitled to the data and that the data should be produced in New York, rather than at a CIA facility. *See* Def.’s Omnibus Mem. 51 (seeking production “to the defendant”); Def.’s Reply 4 (disputing that production “in a restricted environment outside the jurisdiction of . . . the district court” is permissible); *id.* (contending that the unredacted copy of the April 25, 2016 Confluence backup should be provided “in the SCIF”). But there is ample precedent for restricting access to discovery in CIPA cases. In *In re Terrorist Bombings of U.S. Embassies in East Africa*, the Second Circuit rejected the defendant’s argument that the Government’s practice of providing classified discovery to his attorneys, but not directly to him, violated his right to present a defense. 552 F.3d 93, 126 (2d Cir. 2008). The Court concluded that “any interest [the defendant] had in personally inspecting the material was insufficient to outweigh the government’s interest in avoiding unauthorized disclosures of classified information.” *Id.* at 125. That was true even

⁴ Defendant’s expert raises a host of other issues which may be proper arguments at trial, but are not the subject of this motion to compel. *See Bellovin Aff.* ¶¶ 22-23, 27-30.

though the defendant's attorneys argued that "they required [the defendant's] assistance to determine what portions of the classified material provided by the government . . . were relevant to [his] defense." *Id.* at 123-24. The fact that Defendant represents himself does not call for a different conclusion. *See, e.g., United States v. Subasic*, No. 09-CR-216, 2011 WL 1930628, at *1 (E.D.N.C. May 19, 2011) (rejecting a *pro se* defendant's motion for direct access to classified discovery and reasoning that, "[a]lthough a defendant has a right to conduct his own defense, here principles of national security also come into play that do not permit defendant to have access to classified evidence . . . without the assistance by standby counsel").⁵

Defendant contends that he has unique expertise that would permit him to analyze the discovery the Government has provided. That may be true. But it does not overcome the Government's security concerns particularly where, as here, Defendant has a well-qualified, cleared expert and multiple cleared standby counsel with access to the same information on his behalf.⁶ Similarly, Defendant's argument that it is unreasonable to require his expert and standby counsel to travel to a CIA facility to review discovery is not supported by case law. In many circumstances, sensitive discovery must be reviewed in a government facility and there is no law or rule requiring that the facility be in the district of prosecution. *See, e.g., United States v. O'Rourke*, 470 F. Supp. 2d 1049 (D. Ariz. 2007) (finding that the defendant was provided

⁵ Moreover, Defendant was warned by Judge Crotty when deciding whether to represent himself that "a professional attorney would not face the problems you're facing because you're incarcerated" and that he would "always . . . be at a deficit vis-à-vis retained or appointed counsel, who does not carry the burden of being incarcerated." ECF No. 483, at 8-9. Defendant indicated that he was "willing to abide" by "whatever happens" with respect to "[his] access to unclassified discovery, [his] access to legal research, the hours of the SCIF." *Id.* at 4.

⁶ Defendant's argument that he previously had access to the same data while employed at the CIA, Def.'s Omnibus Mem. 51, holds no water. Because he is accused of leaking that very data, it is entirely reasonable for the Government to have security concerns about providing it to him afresh.


ample opportunity to review discovery stored in a government facility despite the fact that his experts were required to travel from Ohio to Arizona to inspect it).

CONCLUSION

For the foregoing reasons, the remaining portions of Defendant's third and fourth omnibus motions — seeking to preclude the Government from using the forensic crime scene evidence at trial or, in the alternative, seeking to compel the production of additional forensic data — are DENIED. The Clerk of Court is directed to terminate ECF Nos. 688, 765, and 793.

SO ORDERED.

Dated: May 24, 2022
New York, New York



JESSE M. FURMAN
United States District Judge